SAN JUAN – NextGen Presentations
Monday, March 12, 2018 – 13:00 to 15:00 AST
ICANN61 | San Juan, Puerto Rico

UNIDENTIFIED FEMALE: …degree in international affairs. I'm currently studying for a graduate degree in computational linguistics, and I also work full time in Washington D.C. in international development and digital education.

ISHAN MEHTA: Hi, everyone. I'm Ishan. I'm in the masters program, school of [inaudible] policy, Georgia Tech, and I'm also a member of NCUC and I'm going to be talking about content regulation and ICANN tomorrow.

DEBORAH ESCALERA: Okay. Well, welcome, everybody. We're very excited to have you here today. We're going to start our presentations. I want to thank specifically my ambassadors for joining us again here at ICANN61. Raphael, Krishna, Joash, Fidya and Sheilla who are going to be great help to me this round.

We're going to get started. I want to thank the audience members for joining us, and our online participants as well. We're going to start off with Savannah Badalich. Savannah.

SAVANNAH BADALICH: Hi, everyone. I'm going to be talking about the role of platforms and the radicalization of white women to white supremacy. A little bit about me. I'm a human rights advocate focusing on technology, gender and extremism. I went to UCLA for my undergraduate. I'm a graduate student studying human rights on the Internet at Columbia University. I have a history of doing gender-based violence activism, specifically as it relates to technology, nonconsensual photo sharing, and I also lead a civic tech startup accelerator at Civic Hall in New York.

My interest in the Internet has been since I was quite young. I as a closeted queer girl in a conservative community wasn't able to express myself or feel safe in my community, and so I found Internet subcommunities as the place where I could experiment with my identity in a safe, anonymous way. And much of my upbringing was actually within a white supremacist community, or at least white supremacy and racism was seen as normal.

And so I'm really interested in the question of how people are normalized and radicalized to white supremacy. And I use "radicalize" in a particular way, because we don't often use "radicalize" when we're talking about white supremacy.

So I started my research focusing on how are white women radicalized to white supremacy on the online platforms Reddit,

Twitter, and YouTube. And I could have picked more popular white supremacist websites like The Daily Stormer or Vanguard News Network – some of them like be familiar from the Charlottesville marches for many folks – but I really wanted to focus on social media because of how ubiquitous it is in our daily lives and how often these platforms are used, and the significance of this – and particularly white women – is because the Internet has been used by white supremacist groups in terms of recruitment since the beginning of the Internet.

Especially in 1996, David Duke, the Grand Wizard of the KKK – or one of them – said, "The Internet gives millions access to the truth that many didn't even know existed. Never in the history of man can powerful information travel so fast or so far. I believe the Internet will begin a chain reaction of racial enlightenment that will shake the world by speed of its intellectual conquest."

This is also the man who brought white women into the KKK for the first time because he saw the power of white women in bringing in their families. So it's really important to talk about white women in this process because they are not just victims or brought in by their partners or friends, they are agents in contributing towards white supremacy.

So my research methodology at first was doing digital ethnographies or scraping people's profiles looking at how and

what are catalytic moments for people to sort of normalize and then radicalize to white supremacy. Then doing interviews as well with current and formal white supremacists, and then also IRL – or in real life – ethnography. Do you want to talk [inaudible]?

My research I did do, I found 15 different profiles, I did two different interviews with former white supremacists, and I kept on coming back and I also made fake profiles so that I can find these people and follow them, I went onto subreddits and I started noticing more about ways that the platform facilitated the radicalization than focusing on how these women were radicalized, so what brought them in, how did they learn about their white identity or the community.

So I started seeing some of these pieces come to fruition. In particular, platform culture and content policies, the way features are used or not used, as well as how people are recruiting on those tools and recommendation algorithms. So my question turned from "How are these women radicalized?" To more of a question of, "How do online platforms' content policies, features, recommendation algorithms facilitate the radicalization of white women to white supremacy?"

So I wanted to keep that gendered lens and I wanted to talk more about the features themselves. This changed the way that I

was focusing on my research. I do have some preliminary findings, though I'm nowhere done with what I'm doing. But I'll start with content policies and culture.

When I say content policies, I mean like the terms of service, for some websites like Reddit or Twitter and YouTube, they have community guidelines. So those are all the policies around what kind of content is allowed and now allowed. Sometimes that relates to spam and copyright, and it also relates to hostility on the platform.

For example, Twitter views itself internally and externally as a bastion of free speech, much of it coming back to The Arab Spring and the rush of activists who use Twitter. But at the same time because it views itself as this bastion of free speech, it does very little proactive work on maintaining its content policies. And so this low priority by the platform itself and the view from the users as well, Twitter is by far the most used platform by white supremacists beyond those specific platforms used by white supremacists like Daily Stormer, Stormfront, the rest, even if they are relegated to the deep web or dark web.

And then Reddit posts certain really catalytic, terrible moments like gamergate, the fappening or all these other nonconsensual photo sharing moments and issues with harassment. They've been incredibly proactive recently with their moderation.

They've enlisted machine learning to instead of waiting for people to flag content, they will actually actively look for it.

And so they have banned numerous white supremacist communities even while I started my research. There was one called r/whiterights that, in September when I first was on the platform, was existent, and then by December was banned. There are other ones like r/coontown or r/incels and all these other ones that existed and now are banned. They also quarantine certain communities that might be more hostile.

Then there are features and functions. YouTube, for example, centers around a channel, it doesn't really have the sense of community in the same way as like Twitter or Reddit, so it gets siloed, but the recommendation function does create a network. Twitter is pithy, it's accelerated, it's stream of consciousness, there are language mutations all the time. So then you see that iconography for white supremacists, like for example the echoes. If you've ever seen someone's name with three parentheses on either side, it's meant to represent a Jewish individual without being caught necessarily by the content policies or any of the bots or regulators.

And then Reddit is siloed to some degree, but their volunteer moderation system and voting systems do create a better-moderated and enforced ecosystem. And I've been giving

praises to Reddit, but Reddit does still have those communities. I still research on there, so there's still a way to go. But they've been doing a lot of really great work.

And then lastly, it's the recommendation algorithms. If you've ever used YouTube, when you click on a video, you'll often see another video that's recommended. YouTube by far is having the biggest issues with recommendation systems. Yesterday actually a techno sociologist named Zeynep Tufekci in the New York Times did an op-ed talking about YouTube as the great radicalizer. And the way that it essentially works is it gets to more and more extreme content each time. And I'll speak more to that in a bit. But Twitter does also have a recommendation algorithm as well. Reddit really doesn't, just the voting system.

So this changed the way that I'm doing my research and looking more at the content policies, looking more at how they're being proactive in their trust and safety work, but I also have some help in ways of other activists who are doing work and researchers around algorithms. In particular, which was brought up in Zeynep's op-ed, AlgoTransparency is an organization by former Googlers – including some people who created the YouTube algorithm – that shows how these algorithms get more and more extreme. And they have on GitHub their code to run the program, and so I've been running the program on queries that relate to these – that I've been seeing that relate to like

white beauty. So one thing that I've seen is the beauty community is a really big gateway for these white women.

So I highly recommend looking at algotransparency.org. They do a lot of really great work. And so for the next steps for my research is just continuing that digital ethnography, continuing doing interviews, testing YouTube's algorithm, seeing if someone has a way for me to test Twitter's as well – so if you know anyone, please let me know – and then just doing that analysis and data visualization.

And then I'll just leave you with one last thing. This is an example of a white supremacist meme, and it is something that you see that's very common. It is filled with white supremacist iconography. It's very gross, but this is the kind of thing that gives you a bite-sized piece of ideology, and people retweet it without knowing because they think it's funny.

So this is the kind of stuff that I'm doing research around. Feel free to do with it what you want. It's both really hilariously badly done and then also it's scary to think how ubiquitous memes are and then white supremacist memes are on these platforms. Thank you.

DEBORAH ESCALERA: Thank you, Savannah. That was fascinating. Thank you so much. Are there any questions from the audience? Let's start with the audience first and then we'll move on to the NextGen.

BARRY LEIBA: Thanks. I guess I have a question about – you led with radicalizing women.

SAVANNAH BADALICH: Yes. I continue to focus on women.

BARRY LEIBA: And your talk didn't say too much about what of all of this is specifically drawing women in as opposed to people in general. Do you have –

SAVANNAH BADALICH: Yes. So I didn't focus on that, I focused more on the features, but some of the things that are bringing in women relate to the beauty community. YouTube has a very big beauty community, and sometimes they post things. There's the #WhiteBeauty that's used by these white supremacists, so sometimes these beauty community people will post that, then recruitment folks from these hate groups will then upvote, share, and they

unintentionally become part of a bigger ecosystem and then it's a way of then networking and bringing them into this.

Same with #ItsOKToBeWhite. There's another one, #TradLife or #TradWife which is traditional life, traditional wife which is talking about previous ways of having family, and then it ends up bringing in these gendered expectations as a way of bringing them into white supremacy. So that's what I've seen. Just very preliminary.

BARRY LEIBA: Thank you.

SAVANNAH BADALICH: Yes. Thank you.

ISHAN MEHTA: Oh. Thanks. Hello. So this was great –

DEBORAH ESCALERA: State your name.

ISHAN MEHTA: Oh. Sorry. I'm Ishan, I work at Georgia Tech, [inaudible] from there. I've looked at the antivaccination movement as an online radicalization method, and the hardest question I thought to

answer there was, how do you define radicalization? Because do they come in with these preexisting beliefs that are then validated in these forums, or do these forums actively change their beliefs? And I was wondering if you had any insight in your work to that.

SAVANNAH BADALICH: Yes. Fantastic question, and one my advisor, Dr. Desmond Patton has asked quite a bit of me. From my view of radicalization, it's from going at the beginning of their profile history from not posting any sort of white supremacist iconography to being self-identified white supremacist. So that's sort of what I've seen as the trajectory.

But from doing interviews with former white supremacists, including Angela King who is a former skinhead and is now an antiracist advocate for the nonprofit Life After Hate – I want to give them a shoutout because they do great work – it ends up being that reinforcement. They already grew up in that language, they grew up with those racist jokes, they have that as sort of a currency when they join those groups, and they find community and identity. And that idea of white guilt sort of melts away when they have someone to blame. So those are the pieces that I've seen as it relates to your question.

DEBORAH ESCALERA: Okay. Let's have two more questions. Go ahead.

HALEY LEPP: Hi. My name is Haley, I'm a NextGen person. Not Fellow. I have a question about the role of moderators in your research. You touched on that a little bit with Reddit. What do you see as being harmful as far as how moderators contribute? And then also helpful.

SAVANNAH BADALICH: That's a great question. Moderation and spam tools can be weaponized by hate groups. They often are and will target people of color, Jewish individuals, activists to bring down their profiles, etc. And certain platforms like Reddit, if you have a subreddit like r/whiterights, it's obvious what the moderators are focusing on. So they will get rid of any dissent and then will sort of create this self-contained ecosystem talking about white rights and white power and identity.

So in that way, it can be actually a reinforcement tool and policing norms, so they are the ones that create norms, police norms, and action norms, and that's very important, and that's a negative way of the moderation. But for bigger subreddits or bigger communities and even weaponized by progressive folks,

moderation tools can be really powerful for combating hate speech and specific violent rhetoric.

So it can be – like any tool, like the Internet itself, it's a utility for both human rights expression and abuse.

DEBORAH ESCALERA: Okay. One final question before we move on? Let's let – go ahead.

CAROLE VODOUHE: I'm Carole, NextGen. I have studied the recruitment for [ICE] by ISIS, and I see the same patterns. You tell me if I'm wrong. And I was wondering if the solution – because I'm pretty sure you are looking for solutions – can it be the solution for ISIS, to fight against ISIS recruitment, can be applied for the white supremacists too?

SAVANNAH BADALICH: Yes, it's interesting because most of the conversation around radicalization online has been around Islamic terrorism, which creates a very narrow role and narrow conversation which is why I use the term radicalization to kind of combat just that view. But definitely. The NYPD – New York Police Department – have done a crime report talking about radicalization and its

antiterrorist work, and it's identical to how these women join white supremacy. They're trying to find an identity, they have insecurities, they find a community, that community reinforces norms, they have that cultural currency that they can then exchange, and then they become more and more entrenched and those norms are more and more enforced. And then by the time they're at the end of it, they're now an active member. So I definitely think that those pieces should be considered. Any sort of violence promotion can be inserted for white supremacy in my research, I believe.

DEBORAH ESCALERA: Okay. Thank you, Savannah.

SAVANNAH BADALICH: Yes.

DEBORAH ESCALERA: Okay. Our next presenter is Jesus Rosado. Jesús.

JESÚS COLÓN ROSADO: Good afternoon to everyone. I'm actually going to do my presentation in Spanish, so I'm going to ask you to please put your headphones.

Again, welcome everyone to Puerto Rico. The Puerto Rican delegation would like to welcome all of you. We're happy to be in our own country. As a government employee and a student of political sciences, I'm not going to get into technical aspects. I know the next presentations will be quite technical, especially the one that will be made by my colleague. But I'm going to give you a more governmental approach what the Puerto Rican administration is doing currently.

Bearing this in mind, I will be talking about the steps taken by the current administration from a point of view of public policy and technology. As an introduction for you to be more familiar with our situation in Puerto Rico – I guess you've read about it – the discussion has risen to an amazing level, especially after Maria storm six months ago. The Commonwealth of Puerto Rico has currently a debt in excess of $70 billion which has seriously affected the way in which the current administration is working and the way in which the budget is allocated.

Based on this, what we have seen in the Ministry of Education and Ministry of Health has been huge, and the current administration has tried to leverage technology which sometimes reduces costs. At the end of my presentation, I will show to you that this is not yet enough and these kind of ICANN meetings help us to advance on these discussions. And I'll show you that Puerto Rico can be part of international community.

The current administration has decided to have the main point of view the economic aspect, but without the economic aspect you cannot do anything because this is precisely what the department allocates money to public policies.

Bearing this in mind, the federal government has devoted money to the island. It's not too much, but it's a first step. Now, what can we do locally? Locally, the administration has tried to promote technology in the different structures, form the most simple areas in the Ministry of Education to the most complex areas in the Ministry of Economy or the Treasury.

I'm going to talk specifically about the creation of PRIT. PRIT is the Puerto Rican Technology and Innovation Service. It's an office that reports to the Office of the Governor of Puerto Rico. You heard him a couple of hours ago, Mr. Roselló Nevares. The executive order signed by the governor is called the Technology and Innovation Services in Puerto Rico. In general terms integrates the other governmental agencies and in a way forces them to become integrated and find ways to facilitate and provide services to citizens through the Internet. It also promotes private capital investments so that the economy will work together with the government to move forward.

Actually, it's a very recent initiative. This administration has been working for a little over a year, and because of the storm,

many projects have been affected. So bearing this in mind, we will go to the creation of the Chief Information officer through another executive order. In a republic, this would be similar to a secretary. This would be the rank. The governor signed this executive order to create a Chief Information officer who will have to integrate technology and promote communications in the island.

I'm going to quote part of the executive order signed by the governor who wants to streamline processes so that they can be up to date with the current cutting-edge technologies and work in accordance with the demands in the handling of information in the 21st century. Mr. [inaudible] was here with the governor this morning.

This is the governor's vision. I'm going to say this in English. I will quote him directly. "For me, it is indispensable that we can count on technology and scientific knowledge so that we can do great things. Our government will be open and want to listen to this sector who help us grow. We do not want to be a further obstacle in technology and innovation as the opportunity to create a better Puerto Rico."

We may not know this, but the governor had a chance to study at the MIT in Boston and it was this experience that made him promote the same things in the island. He wants to develop a

wider technology environment. Currently in the island, if you want to pay taxes for example, in the past you would be able to do this over the Internet, but this has only existed for a short time because further back in time, you had to go to the bank to pay your taxes.

But there is now a public policy integrated with private sector, the banking sector. Now the goal is to do away with tax collection offices at the municipalities where in the past you would go and stand in a queue for 30-40 minutes to pay maybe a speeding ticket. Now you can go and pay at the banks or over the Internet.

Which are the main technology issues identified by the Puerto Rican government? What has the Puerto Rican government faced? The first issue is always security. Official governmental sites are quite weak, quite vulnerable. We should also point out that there is a very slow technology implementation in the governmental agencies. Since this implementation process is so slow, the citizens suffer from this. And the third issue which has been identified is that the industrial sector has not been willing to cooperate with these projects.

At the end of my presentation, I will e-mail to you through our group chat an initiative that was mentioned by the governor this morning. I worked on it myself. And we want citizens themselves

to be able to report to the government what regulations they consider should be done away with because they are too expensive. For giving you an example, the Treasury department now, some procedures can be done over the Internet, and they work with the municipalities so as to increase their tax collection.

The general opinion of citizens is that the government is not efficient and it is too slow. There's still a lot to be done. As a civil officer, I can tell you that lots of things are being done, but because of the storm, many things have been delayed. In Puerto Rico, there is a serious government transparency issue. I cannot deny this. Access to information is restricted, and it's always been an issue for citizens. But it's this type of fora such as the one we're participating in where you find opportunities. We want the Puerto Rican government to join international discussions so that it will become more efficient and streamlined so that we can provide services to citizens who are the ones who pay taxes. I'd like to thank you for your attention, and if you have any questions, I'd be more than happy to answer them. And right now, I will send this initiative, the "cut the red tape" initiative to you. Thank you very much.

DEBORAH ESCALERA: Are there any questions from the audience?

UNIDENTIFIED FEMALE: My name is [inaudible] I work as a youth representative at the United Nations on their [inaudible] 365. I was part of the recent meetup for blockchain, and one of the things that we're implementing is new technology in obviously the government situation here in the system and the political system here in PR for civilians. I asked this question already, but unfortunately what I got was an answer that was not sufficient.

I work a lot with youth, and since we're talking about youth issues and the government, my question is this. Are there going to be any programs implemented for the youth to learn about these new technologies for future job applications or to work in the government in the future?

JESÚS COLÓN ROSADO: Okay. And that's a really good question. I'm going to answer it in Spanish just to make sure that I really get to it. At present, the problem that the young people find in becoming integrated to the government is an issue. It's a serious issue. The initial issue is that the youth do not work in the government. If you go to any agency in the country, the average age of civil servants is 40 to 55 years of age. I'm talking of people who in four or eight years' time will retire. And it's precisely these types of issues that show the performance of agencies.

The house of representatives has been attacked because people would say that they would only grant contracts to older people or to people who are part of the same political party. The House of Representatives went through this process, they added to their website this link where you can see what jobs are available. In order to go straight to the point, no, there are no initiatives and there may not be these types of initiatives in the near future.

There's a lot to be done form the point of view of public policies, the youth and technology. I think it's ridiculous for me to have to go through a bank to pay taxes or stamps so that I can use my car every day. There are many initiatives in the municipalities, for example. There are similar issues. The Puerto Rican population in ten years' time will become much older. We will have a population of older people. We need more youth.

Is it good to do business in Puerto Rico? It is. You have the right environment to do business. Puerto Rico is very competitive as compared to other areas. I think it's one of the few things that the current situation offers, but there is a lot of room for improvement, and undoubtedly, this is a challenge that the current administration is facing. And youth leadership, I'm sure that many of you will become leaders in your own fields and many of the challenges you will face will be related to this. How can I join the discussion as a young person, and how can I

contribute new ideas for the government to be more efficient and to offer better services to citizens?

DEBORAH ESCALERA: In the interest of time, we're going to need to move forward, but thank you so much for your presentation.

JESÚS COLÓN ROSADO: You're welcome.

DEBORAH ESCALERA: Well done. Okay, we have a special guest who would like to say a few words to the NextGen, Sally Costerton. Sally?

SALLY COSTERTON: Hi, everybody. Thank you, Debs. I don't think I'm a special guest. I think I'm probably a rude guest, actually, bursting into your meeting like this. But I have overall responsibility in the executive team in the ICANN org for this program, and we have challenges often with the agendas at ICANN of all coming to these meetings, but I wanted to take the opportunity to introduce myself.

I work with this wonderful lady here who we are tremendously lucky to have at ICANN. She has enormous passion for this program, as I know you will all be aware, and she has passion for

it because she believes, and she sets us all a very good example. In ICANN's mission, she believes in the critical role that this program plays in helping ICANN to deliver its mission. So by being here, you are playing perhaps a more important role than you realize in helping ICANN to deliver its new mission, its new bylaws. And specifically the part of – if you like this sort of thing, go and have a look at the mission and the core values and commitments part of the mission.

And in there, it gives us some instructions – and they are instructions – and they say that it is our job to ensure that the world's Internet users' voices are heard in the ICANN process, and that that needs to be done in a bottom-up, multi-stakeholder consensus model – that's a second point – and that therefore we need to ensure and we need to make great efforts to bring people from all over the world but also from different backgrounds, people with different views, people of different races and ethnicities and religions, so really, truly diverse contributions in every way that you can imagine, really. And then it says something else, which is the other part of this program. It says that they must be able to participate in the work of ICANN.

So it's not just about showing up. And you're here for the first time, you're showing up. And thank you for that. Some of you will have come from many thousands of miles away to be here,

and this is fantastic to have you here. This is a big region. Saying, "Hey, this is a regional program" doesn't mean it's ten minutes on a bus ride. So thank you for the time that you've given to this program. You're busy, you have studies, you have busy lives. But my message to you is, don't just show up once. Participate. And if you think that we're not giving you enough skills, it's partly about knowledge but it's also about how you work at ICANN. How do you find the right people to talk to? How do you learn how to ask people for help? Harder than it sounds, actually, sometimes.

And my team are here. Anyone you see at this meeting who has one of these badges that says ICANN org, the pale blue label, we are the ICANN staff in more conventional language. And that means we're here to help you be successful. That's why we're here. That's what we do. And Debs is particularly focused on this program, but we are all here to help you to participate in ICANN to help it deliver its mission. So I just wanted to introduce myself and say that you're very important people in our world because you carry with you a lot of expectation for the future from the communities that you come from.

And it's our job to make sure that you leave this meeting really well-equipped to take that message back to your communities, your universities, into your academic studies, into your networks so that we can, between us, expand the contribution of the

world's Internet users to the work that ICANN does and that really important work, the role that we play in supporting the internet.

So I just wanted to say that. And if anybody has any questions for me – I don't know if Debs will let you ask, but I'll give you a couple of minutes. I'd be very happy, and as they say in comedy, I'm here all week.

DEBORAH ESCALERA: Okay. Let's move on with our presentations, and next up is Justin Cray. Justin.

JUSTIN CRAY: Thanks. Hi, everyone. I'm Justin Cray, I'm a masters student in computer engineering at Cornell University, and there I'm focusing on computer networking and Internet architecture, and so I figured I'd talk about that in the context of IoT and try to talk about some of my projects I'm working on there as well.

Just briefly about myself, I like engineering because we get to design systems that just work. So when it comes to creating the backbone of the Internet, when we say "Just work," we're trying to make the Internet here scalable, modular, adaptable and standardized that as new ideas and new products form, they can just plug themselves into the Internet.

What that means in practice is that the end user may not know what's going on behind the scenes, but people like us who are here spending our time trying to figure out how can we build a system that just works for the Internet end user. So I'm excited to be here and see all of this going on.

But enough about me, we'll talk about IoT a bit. IoT is really this big emerging industry, and estimates vary. [We'll see] about 25-50 billion IoT devices on the market by 2020. What that means is there'll be more IoT devices than there will be regular phones, laptops or desktops. So this is really a tremendous addition to the infrastructure that we see today, and there's also a large global market value in that as well.

And really, the nifty part about IoT is that it really goes everywhere. The classic examples you'll see are in cars or in buildings or things like this, but you can really stick an IoT device in anything and add some additional functionality to it. And that's what makes this such a large-scale project.

And IoT has several unique challenges. Effectively, how most IoT systems work now, briefly, is you see a bunch of different devices hooked up to some sort of aggregator, and this aggregator is the facilitating communication between all these devices, and that gets hooked up to the worldwide web.

What that means in practice is we see a bunch of different issues emerge. The first is really that IoT's big. So you're seeing that because you had billions upon billions of devices scattered all across the world, you need the network infrastructure, number one, to have all these devices connected to the Internet, and that's not there in many particularly developing regions or even like in developed regions where you're trying to put sensors in environments that aren't served by Internet.

You also need software and hardware to manage devices, and also collect the data. Once these devices are spitting out data, you have trillions of data points that you have to manage and figure out, "What is this useful for?" And also, how do you facilitate this with kind of the larger Internet infrastructure? And this is really where a lot of the naming and addressing – and particularly IPv6 – comes in handy, where as you add more and more devices, the Internet needs to scale accordingly.

But IoT is a separate set of challenges which is IoT is small. We're building these devices that are very low-power because they're running off of batteries and they're not running off of power supplies, they're low memory and they have limited processing capabilities. So you want to be able to stick these IoT devices in noninvasive areas that aren't adding tremendous amounts of power or other requirements to your system, and so you have to create the infrastructure to not only handle the big picture of IoT

but also make sure that these devices which effectively have very little computing resources are capable of handling this.

So to be able to scale up in that work, we're also scaling down the burden for the individual devices, which is quite the tough challenge. So I'm going to talk about a number of solutions that have been developed for this on the Internet architecture side of things, and then discuss how that can play into the bigger picture of some work I'm doing.

The first thing I wanted to highlight here is lightweight IP or also known as micro IP, or these are different variations of kind of the same thing. And the idea is to implement the whole network stack – so all the way from the physical layer to interfacing with the application – on an 8- or 16-bit microcontroller. So we're talking about tens of kilobytes is the size of this code here.

And this code is great because you can fit the entire network stack on a chip that's the size of your fingertip. And this really allows you to have these different devices placed in locations where you won't conventionally see computer systems because of size requirements and power requirements, etc.

And the real innovation here as I highlighted in the slide is the one-packet buffer. Typically, how these devices work is you're storing dozens, hundreds or thousands of packets inside of a device that connects, and it will send some and then it'll have to

retransmit some. This whole back and forth depending on what protocol you're using.

But really, this system is designed in a way so you're only storing one buffer at a time, on both the send and receive end, and this allows that low memory requirement I mentioned earlier but creates a whole slew of complications. This technology is developed by Cisco and I believe folks in the Switzerland Institute of Computer Science as well, so it's an exciting time.

Another thing I wanted to highlight is 6LoWPAN, and this address is a solution designed to address concerns in terms of developing – interfacing these networks that are wireless personal area networks. So the idea behind this is that you have a bunch of devices that are connected together in the same local network to each other but aren't interfacing with IP directly.

So you'll see on the slide – there we go – the red circle area is a bunch of different IoT devices that are not connected over IP. They're connected to each other through this protocol I'll highlight in the next slide, and these all interface with an edge router, and that edge router translates IPv6 messages from IPv6 which is too much of a burden for these low-memory devices to a smaller packet, effectively, which can then be distributed amongst these different areas, devices in this WPAN network.

And so what that means in practice is this is built as a way to interface with IEEE 802.15.4 which sounds really boring, but it's basically a protocol for these low-rate WPAN networks. So this is designed to address systems where these devices may not frequently have an Internet connection, may have a really slow Internet connection – not like 2G, like ridiculously slow Internet connection – and also have unreliable – and also have the same issues as before where they're low-memory and not a lot of processing power, etc.

And so basically, what we're doing here is we're trying to take the IPv6 infrastructure that powers the entire web currently and interface with that. And so this protocol is going to kind of remove some of the unnecessary parts of the IPv6 packet, and also other different layers as well. So you're getting rid of some header compression, getting rid of some unnecessary header information, taking a larger packet – the 802.15.4 packet has a maximum size of 127 bytes, versus the MTU of IPv6 is 1280 bytes. So you have to take the big packet and divide it into smaller packets, and make that not a problem for the person on the other end who has no idea that this whole thing is going on. They're just using IPv6 to go talk to you.

And also stateless autoconfiguration which is a new part of IPv6 to avoid the DHCP to automatically get that address signed. [You

just don't] want to have this kind of IPv6 functionality built into these networks.

And also, the last thing I'm going to highlight is this web of things idea. Right now, the Internet – the web, I guess – is powered by all these great technologies, HTTP, XML, etc. And these are all standards that were not built with IoT in mind. So there are folks out there in the IETF and also in W3C – which is another standards kind of board – that are adapting these technologies to be lightweight so they're accommodating these kind of devices. And so it's also interesting because of the nature of IoT devices where typically, things like HTTP are structured in this kind of request-response architecture. So you will say, "Okay, server, give me this information," or, "Okay, server, I have this information," and the server will respond.

IoT devices are mostly event-driven. Something will happen, it gets triggered, and then that's what really requires the attention of the network. And so leveraging that, folks, we develop standards to kind of adapt this which are more lightweight alternatives to HTTP. I'm highlighting CoAP here. And this maintains a lot of the subset of the HTTP methods so you have GET, PUT, POST, DELETE, whatever, but it's really designed to be lightweight and has binary representations of these. And so that's really great, where it kind of again strip out some of the

unnecessary parts to not overburden the infrastructure of the network.

And going off of this, you have DNS-SD which is going to kind of help with the services exchange there, and also DTLS which offers encryption services for these UDP networks. And trying to just offer a summary here. I know I threw a lot of jargon out there. On the left side, you'll see different layers of the Internet. So if you're familiar with this, the network stack, effectively, and I'll go through it quickly.

The physical layer remains unchanged. We have no control over the physical layer in a lot of these protocols. The data link layer, instead of using 802.11 – which is Wi-Fi – or other kind of things like this, or ethernet, you're using these data link layers that are designed for situations where you may not have frequent communication and may not have high-bandwidth communication.

Similarly, IPv6 is kind of an inevitable track for the network layer, and so you're seeing things like 6LoWPAN emerge, kind of adapt IPv6 to these resource-constrained devices, and then these typically use UDP because again, TCP is a lot of overhead. And then on the application layer, you see a bunch of different things, but you want to make sure they're kind of building off

these REST APIs. So we're modifying stuff like that to kind of adapt to the situation.

I'll talk a little bit about some work I'm doing up at Cornell with my advisor, Dr. David Schneider. And the idea behind this is that building technology is a very exciting application of this, where you can effectively mount these IoT sensors in any building that currently exists and start gathering information about the building itself, so occupancy data in rooms, temperature, humidity, etc., and then you can plug all this information into a machine learning algortihm – which is not my area of expertise, unfortunately – and then control heating and cooling systems amongst other things in the building using all this data.

So you want to take a building built 50-60 years ago, stick a bunch of sensors in the building that are not requiring a whole electrical infrastructure overhaul but are powered by batteries and are not particularly – or may not be in a highly accurate or well Wi-Fied area, you can kind of build out this infrastructure using the aforementioned protocols to allow retrofitting of old buildings, saving energy and cost and all these things using some of the aforementioned infrastructure. So really, there are so many applications, but this is the one I'm working on to kind of understand better how we can leverage these technologies and leverage these existing protocols to make IoT possible and change the world.

So my last question is, what Internet architecture and what protocols and ideas need to be developed so that we can accommodate the next big thing? So as society progresses and more and more people think of ideas we can't even conceive of right now, what needs to be in the backbone of the Internet to accommodate that big thing?

DEBORAH ESCALERA: Thank you.

JUSTIN CRAY: Thank you.

DEBORAH ESCALERA: Okay. Let's go to the audience for questions and then to the NextGen. Are there any audience questions? And then Shamar, we'll come to you.

BARRY LEIBA: This brings me back to something I said for the first NextGen presentations I went to in Johannesburg which is what got me hooked. You guys are the ones who are going to come up with the next big idea. I've been doing this for 35 years. I have no idea what's next. I'm looking at what we've done and I'm amazed at where we came. And we came there because back when we

were your age, we were brilliant, and now we're grey-bearded. But you're brilliant, and I just want you all to think outside the box and prepare us for the next big idea and come up with it. That's all I had to say.

DEBORAH ESCALERA: Thank you. Shamar, you had a question.

SHAMAR WARD: Good afternoon. Shamar Ward from Barbados. Thank you for the presentation, Mr. Cray. Very interesting. The only question I have is about using UDP only at the transport layer. We know UDP normally has a very problematic transmission, problems in terms of packets being lost and information not being transmitted correctly. So when we are looking at IoT devices which might be dependent on say, for example, dispersing water if there's a fire, you may not want to use UDP which maybe not only just have packets dropping but be unsecure. Do you have any ideas on how you could address that?

JUSTIN CRAY: Yes. So the short answer is you're right, of course. There are different applications of IoT devices, and so if you're looking for reliable transmission, UDP is not the protocol for you. There's no getting around that. And if you have applications like you will

have with IoT where you need reliable transmission and you have to use TCP and kind of accommodate the infrastructure and the overhead on the device side that accommodates that, there are comparable methods of encrypting both. Those [I can go off for] different time, but the short answer is, yes, you're correct. You have to have some abilities to handle reliable communication for a lot of applications.

DEBORAH ESCALERA: Okay. Go ahead.

HALEY LEPP: Hi. This is Haley, also NextGen. Great presentation. I'm really intrigued by how you ended talking about retrofitting a house with this infrastructure.

JUSTIN CRAY: Thanks.

HALEY LEPP: And it made me think I often work in areas that are either not developed with Internet infrastructure or face destruction of Internet infrastructure either for something like Puerto Rico that has had a natural disaster, or places where there's high levels of conflict. Do you see that this sort of new technology would be

applicable in these areas? And what would need to happen to make this environment amenable to this tech?

JUSTIN CRAY: Yes, absolutely. So then the big question here – and this is kind of a big ICANN issue as well, and I guess also ITU thing – is whether you have Internet. Because if there's no Internet here, we're in a whole separate issue where these devices can't talk to the outside work because they're kind of trapped on a local network. If you can deploy that in an unreliable way, we can kind of accommodate that into infrastructure working so you may not get every packet through the network, but that is a big issue where you need to be able to build out these things.

There is a method of having like local networks talk to each other, kind of like an ad-hoc network, and that can be considered I guess an application of IoT in a way, but really, IoT involves connecting to what we would define as the Internet to kind of make things work. So having these sensors mounted in developing countries would allow for a whole slew of applications just in terms of data collection to even inform better decisions going forward as to how you worry about environmental issues or human rights issues, etc., and that's a great application of this technology, definitely.

DEBORAH ESCALERA: Okay. We have time for one more quick question. Go ahead.

ANNA CECILE LOUP: Thank you for a wonderful presentation. I'm actually interested in – you talk about sort of this idea of moving forward, but I'm really interested in who's in the room when these sort of new – how to approach these big ideas are coming about. Because if we think about the history of how technologies are developed, there are choices that are made. So I'm interested in just hearing really quickly about sort of your lab and who you're working with, and sort of what the dynamics are in the room. Is it driven by sort of the up-and-coming NextGeners, or do you feel like there's a sort of [call in] response between those who have been in this space for a bit longer? I'm just interested about sort of the lab experience you have in developing these sort of new technologies and approaches.

JUSTIN CRAY: Yes. So we don't develop the protocols in my lab. The protocols are actually developed by organizations like the IETF and the W3C which tend to be a lot of folks who've been involved with the Internet since the beginnings, which is a whole separate conversation. In terms of the application of the technology, you do see a lot of people in this space, in IoT in particular, who are kind of pushing this from the younger generation, because a lot

of these devices kind of fit in the startup-y model where someone is making a small little chip and that chip [inaudible] the Internet in some big way.

And then the other big player in the space are the big networking companies like Cisco which again have a whole range there as well in terms of kind of the diversity of people involved. So it's a tough challenge. Academia also tends not to be the most driven by the younger, more entrepreneurial generation, so it's a mixed bag.

DEBORAH ESCALERA: Okay. Thank you so much, Justin. Fascinating. Okay, our next presenter is Fransleidy de Jesús Díaz. Fransleidy? Are you going to present in Spanish?

FRANSLEIDY DE JESÚS DÍAZ: Yes.

DEBORAH ESCALERA: Okay. So headsets, everyone.

FRANSLEIDY DE JESÚS DÍAZ: Hello. Good morning, everyone. I'm a student for National University College, the [inaudible] Maria. I study nursing sciences here in Puerto Rico.

My presentation will be about the electronic health record. Medical files are confidential and secure records. They're records about healthcare treatments provided by doctors or healthcare providers that are stored in a computer. If healthcare providers use electronic records, they can join a network that will share records in a secure manner. Some of the advantages of the electronic health record is that they're trustworthy, easy to use, fast, modern, low-cost with a low monthly payment without an upfront investment.

Here in the United States, the HITECH Act has been implemented to protect data confidentiality. According to this act, we get money, funds to take all records from hospitals and transform them into electronic records by 2020. All hospitals in the U.S. will use electronic health records. There's a very important element. These records will be accessed by people all over the world. That is, anyone from any part of the world will be able to access these records. These records will be updated continuously, and data will be in a secure platform.

Another advantage of the software model is that there is a website where any issues can be worked out. And you don't need an additional software on your computer. You only require Internet connection to use the system. The data are stored in a secure platform. Furthermore, all data are backed up. There are three different types of records. Every country will have a

specific record with their corresponding data. This will help us reduce medical errors, duplicate information, and this will also improve quality of service. Costs will be reduced too.

On paper, information is not secure, information may be duplicated, and in this way, we will avoid this. There is an important element. Not everyone knows how the information can be protected. And it would be good for people to know what the ICANN is doing. It is good that ICANN helps people communicate over the Internet and that data can be stored and accessed through a web address.

People should know that ICANN manages these unique identifiers. Without this coordination, we will not have a global Internet. So the electronic health record aims at having all nurses, hospitals, healthcare providers share the same data, because all these players are working with lives. And those lives may be your relatives, may be any person. If you travel to another country, the doctor who will see you in this other country will be able to access your information, information about the medication you take and about your diseases. This is the goal. We want information to be good, secure, reliable. Because not everyone has information on paper.

On paper, information may be interpreted in different manners, while if you have a secure data record, you will have a common

language. And if you do not understand the language, you can have it translated. In summary, nursing processes have evolved. Healthcare professionals should be updated in terms of healthcare and electronic records. We need to interact with all of the different players, and depending on your need, you will have to update the electronic systems.

So you need to know what you need the information for. In Internet, we'll have Internet governance. This will have to be necessary. And we will need Internet for the whole world.

DEBORAH ESCALERA: Are there any questions? Go ahead.

KAITLYN KARPENKO: Kaitlyn. I'm part of the NextGen program. So when you're thinking about electronic health records and the way we transfer it over the Internet, do you view laws like HIPAA or other laws that affect the way you can store and the way you're supposed to treat medical records as helping this or hindering this? How do you view laws that treat medical records in a special way in the context of electronic health records?

FRANSLEIDY DE JESÚS DÍAZ: HIPAA act is one act, and there is another act that's called HITECH which regulates electronic records. The goal was to provide support to the HIPAA act. What happens with this act? You have to encrypt the information that you transfer from one computer to the other, so not everyone will be able to access the same information. You will be able to send this information from one computer to the other. An IP will give you that security, but you will also have to encrypt that information. Those are the two elements of the electronic health records.

[Overall,] three different types of records. Depending on the countries and depending on Internet use, you will be able to access these three different levels. There is also a web office that will be available to solve any issues 24 hours a day.

DEBORAH ESCALERA: The audience?

UNIDENTIFIED FEMALE: I am [Filomena]. I'm a representative of the youth for United Nations 365 program. My mother is a nurse here in Puerto Rico, so this is a personal question. Many years ago, a system was created to collect patient information, and as far as I know based on my experience, many nurses were having many technical difficulties. Even though they were continuously

trained, they had a hard time in using technology. So I'd like to know whether you're going to implement a program to help these people who are not trained and do not have the necessary computing skills.

Part of the implementation of this electronic health record is threefold. It's not that it's going to be implemented overnight. First of all, you need to train the staff so that they will be able to use the electronic health record. The staff will be trained, and you will also have to make sure that the information transmitted is the right information. So what happens with the staff? Some members of the staff who are older or who are having a hard time with computes will be trained using images. They will use part of a body, they will have a more specific approach in nursing. Not only will they be trained, but there will be special people, those who created the electronic health record, who will be providing training courses to every hospital so that all the staff will get the information, and they will be assessed. By 2020, everyone should have been trained. In Puerto Rico, 27% of hospitals are already using it. The rest is not using it.

DEBORAH ESCALERA: Thank you so much for your presentation. Okay, our next presenter is Juan Rosado. Oh, another Rosado. I just realized that.

JUAN A. FIGUEROA ROSADO: Hi, everybody. My name is Juan A. Figueroa Rosado. I'm a local here in Puerto Rico, and I'm a senior at the University of Puerto Rico. I'm currently [pursuing] my bachelor's degree in computer science. I'm going to be giving you a brief overview about big data and its relevance on the Internet, and after the presentation ends, I will talk a bit about how security plays a role in this.

So this will be the content of the presentation. I'll give a brief overview about what is big data, the key characteristics that compose big data, the implementations that are being implemented by different organizations and research facilities, and my related work that I already did in the field.

So, what is big data? Big data basically is data that we couldn't process on our traditional management technologies. As you know, there's a law that's called Moore's Law that says that the size of our devices and the memory keeps growing exponentially throughout the years. So right now, we're getting to a level that we are being able to manage this data.

To tell you a bit about big data, first I have to give you a bit of insight of the size of data that is being produced. Expected by 2020, we are going to have produced an amount of 44 zettabytes of data. That will be expected to be produced by 2020. To give

you insight of this and the magnitude of the size of this, this amounts to 167 million copies of the Encyclopedia Britannica. And to us youngsters who are always watching Netflix, it amounts to 23 trillion hours of ultra HD streaming. And this is according to the Internet Data Corporation, of course.

This was a transition slide. There's a bit of a format issue from the presentation being imported on different platforms. So this was just a transition slide. So this will be the key characteristics of big data. It's called the three Vs. There are more Vs, but these are the more important ones of big data.

One of them is velocity. Social media and geolocational data that's been produced at a big magnitude, a big speed, and we are trying our best to keep up with that rate. Another V would be variety. It comes in structured or unstructured forms. For example, data being generated from sensors can be coordinates or just signal or frequency data, and the unstructured will be social media information like tweets that we have different processing terms in order to acquire that information. The other would be volume. Data is increasing exponentially as well as right now – as Justin said – IoT. Those devices are producing data, so as more devices are being generated, more data will be produced.

So how do we process this data? There's something called a computer cluster. A compute cluster is basically a lot of computers tightly connected – or loosely connected – that act as one system. So basically, all of the different computers that are connected act as a node, and each node has a task. But since they're all connected, every node has a task and it's being worked on simultaneously. So this will exponentially speed up any program or algorithm you're trying to run.

These are the types of implementation that can be done with big data. Scientific data. There's a lot of data that's being produced on different scientific sensors such as satellites, tidal sensors that represent water temperature or the sea level rise in the ocean, and that data is being processed quickly and we need the [terms] to fix those and actually process the data. That's a big issue, especially with satellite data.

So we talk about financial data, stock market. How is the market moving? How can we make a certain target to people buy stuff? Like Amazon, they keep target advertising stuff and you suddenly find yourself buying it. Also, streaming data, your Netflix, all of that recommendation comes from you watching stuff, on YouTube especially. And the Internet data that comes from your cookies, from your browsing, all of that information that is being generated as you surf the web, the browser keeps

all of that information into account and it's being saved to the company that provides you that browser.

So implementations, as I talked to you, sensor networks that can be in a forest just to study the habitat of different animals and how the ecology is working, or sensors in the water on buoys that they just record information on the water, the temperature, how the wind [getup] is translating to the water and all of that. Also, browser cookie processing. That's basically how you find yourself on Facebook and suddenly you find your favorite shirt and you find yourself buying it later. And geolocation processing. Of course, this is data that's being right now even generated from your phones. They know that you're in Puerto Rico, and that information can be actually processed in order to provide traffic optimization. That's how Google gives you the best routes when you're traveling.

I think this is my work, but it's not showing. Yes, this is my work. The title was on the slide before, but I guess formatting issues. So the research that I did at the Missouri University of Science and Technology where my friend and I did an internship last summer, it was called multi C-Tree Party-Based Clustering on Semantic Trajectories. I know, very complicated title. Don't worry about it, I'll explain it right now.

So basically, what we did, we created a two-round Hadoop algorithm. Hadoop is basically a computing paradigm that helps you implement a computer cluster to process data more efficiently. First, what we did is we took geolocational data. What we did with the geolocation data was we artificially created it first because there was a certain issue asking data providers for geolocational data of their clients. Of course they wouldn't be able to share that with anybody, that's illegal.

So we just artificially created the data by running a Python script and then clustered it with a data structure developed by a graduate student at MST called Katrina Ward called a cluster tree. Those trajectories, we converted them from basic coordinates to semantic trajectories or [knows] which we like, "Hey, I've got this coordinate." We just convert it and it would say like, "Bank, school, you went to your gym." And of those trajectory, we would cluster them, and at the end we would have information regarding all of those trajectories. And that would regress to like 75% of your people went from school and then to the gym. And that will give you some information from your community or from wherever you're extracting your data.

We did this with semantic trajectories so we wouldn't break any confidentiality laws according to the different data providers. So at the end, all the data would be encrypted. That's why we didn't ask first the different trajectory data from the companies,

because first, we would need to actually get in an agreement on what encryption scheme we would use for them to share the data without breaking any laws, and for us to process it without even knowing what data is being processed.

That part of the project is still in the works. I'm still working on it with the university remotely. So that's what my [inaudible] to the community in big data is about. So there are the acknowledgements, of course. The research was worked at the Missouri University of Science and Technology, and to my university for providing me with the tools able to be a part of this, of course. It's an honor. And these are the references where I obtained the data from, how much the data is produced and stuff like that.

So before I go to any questions, relating to this issue with big data, there is a big security requirement that we need to meet. Of course, we have this data and we found a means to process it, but as you saw in my research, there are a lot of security requirements we need to meet. That's a big issue, and in a [probability] like for example, I took geolocational data, you don't know if the data providers are giving your data. For example, Google is implementing these big data solutions, but with their data of course.

But the beneficial part of this is if we try and develop secure implementations with big data, we can actually get a lot of meaningful information from our communities. For example, we can actually determine what areas of a community need a hospital. Like for example, let's say if you study a community and you see that 75% of people have to get a 45-minute drive to get to a hospital, you can determine that the community needs a hospital nearby.

And these solutions – and many more that can be developed by different computer scientists – need security, and of course, this comes with the policies that are being discussed right now. For example, you can't run these studies if the GDPR thing that's coming in May will restrict information and can actually restrict the world from very good implementations that can help them too. So yes, that's my presentation.

Thank you for paying attention. I will try to provide the actual presentation with all the formatting. I think Deborah is going to upload it, because in the screen there is not all the cool pictures I included on mine. So thank you. If you have any questions, feel free to ask them now and I'll answer them as best as I can.

DEBORAH ESCALERA: Thank you, Juan. Okay, are there questions from the audience to start with? No? Okay. NextGen? Anna?

ANNA CECILE LOUP: Thank you so much for your presentation. It was really fascinating. I actually have a question. I do community work back in L.A., and so I'm really interested in this last comment you made about thinking about big data and how it can inform sort of local projects, this idea of if people are having to go 45 minutes to a hospital, should we build one in the community? And I'm interested in your opinion about the role of big data in this type of community development when we're thinking about access to these kinds of technologies. So, is big data used in conjunction with sort of the work I do where we're like on the ground doing interviews in the street, working on the ground with people, or is it something that's supposed to expedite this process? I'm just interested in sort of the dynamic that that would play in community development. Would it be in conjunction with, or would it be a way of sort of replacing the very time-intensive boots on the ground work?

JUAN A. FIGUEROA ROSADO: Most of these implementations would actually come from indirect data processed from different devices. Of course, here in Puerto Rico, we actually got our connection established a month ago fully, so in these kinds of situations, big data just wouldn't help because right now, the big issue we faced after the

hurricane was contacting our loved ones and moving. And even though we are getting back on our feet, it was a very inefficient way of handling things.

And of course, this comes in hand with the government, how they handled everything. But let's say in a very developed country like the U.S., you go to a state and then you can actually help them according to this data that they're producing, and they know they're not going to use it afterwards. So we as a community can actually give them the solutions that at the end will provide a better economy, it will help the community, and at the end, it will give a better life to the community and the whole world, and these are applications that you can expand in different countries. And this is something I would like to promote, finding new implementations, find the permits and all that and able to help the different communities.

ANNE CECILE LOUP: Thank you.

DEBORAH ESCALERA: Okay, any more questions? Go ahead.

UNIDENTIFIED FEMALE: Hi. Great presentation. I have a question. I was really intrigued by your talk of clustering for your project, and it made me think about the way that we're currently analyzing natural language. And I was curious – I know in natural language processing, one of the biggest things we're looking at is neural networks and unsupervised learning to create these clusters. And I was wondering if that ever came up in your research or if that's something that sort of intersects with the field.

JUAN A. FIGUEROA ROSADO: It certainly does. That's something I really want to research hopefully if I can continue my studies after this bachelor's degree. And yes, they come into play. If we develop a certain algorithm and create a neural network along that, that could work with the results of this information. So actually, we could get the data, process it with the algorithms already developed, and run them. But first, we would actually go to a learning phase in the neural network so when we actually give the real test with the real data, we get accurate results. And yes, this plays a big role.

And there are a lot of implementations for neural data. For example, traffic optimization. At first, you can give it artificial data, and the neural network and [itself programs] how often the lights cross and don't cross so there's less traffic when you're

traveling there. So yes, it's a big deal. All of these fields actually cross on each other and have an application in each of these top fields.

DEBORAH ESCALERA: Okay. Yes, go ahead, Savannah, and then we'll go to Shamar.

SAVANNAH BADALICH: Okay, great. Thanks for the presentation, it was great. I'm curious. I loved how you spoke about security at the end, and I'm wondering if you could elaborate a little bit about any conversations you're hearing about the way that big data could be abused or misused by state actors as it's related to human rights defenders, journalists or particular ethnic or demographic groups in terms of targeting. And if there are standards and ways or at least a community of norms that would prohibit this kind of use. Hopefully I asked that question right.

JUAN A. FIGUEROA ROSADO: Yes. So yes, there are ways that big data can target different communities. For example, I talked about unstructured data and how that comes from different social media websites. I could actually develop a web crawler with an algorithm that can extract meaningful data from the different tweets within a certain community, and from that, I can extract the information.

For an example, you have a community that's going to do a march, and let's say it's a beneficial march, whatever, but this data can be processed, extracted without your knowledge and sent to different – I don't know – communities so they can actually like boycott your activity. So yes, there is a security issue. And that's something that really should be worked on, and I would really – later on in these four days – ask different representatives from the security aspect of ICANN and ask them about these issues, because it's a field I'm interested in, but in a good way. There are a lot of people who can use this information in harmful ways. So that's my mission for this week. Thank you.

SHAMAR WARD: Thank you for this presentation. I don't have a real question, it's more of a comment. I'm seeing that Puerto Rico and also other Caribbean islands were affected by severe catastrophic hurricanes. The use of this information and the approach which you have suggested may actually be able to help us better understand how to better not just prepare but to actually understand the behavior of persons when a hurricane may be coming to see if persons are actively becoming prepared for such an activity. So that was just maybe a suggestion even so.

JUAN A. FIGUEROA ROSADO: Yes, it is. For example, first we had Irma, and that hurricane just gave us a big scare. It basically just glanced off the coast, gave us some rough winds, but that was about it. And at first, when that came, the community was not prepared. Everybody was taking it as a joke because we're used to hurricanes, we're in the middle of the Caribbean. And then when Maria came, people were like seeing the actual hurricane coming and they're like, "That's not going to hit us. I promise you." And it hit us, and it destroyed everything.

So I hope that the community learns from this and that this different implementation can actually help us determine how after a natural phenomenon like this, is the community taking this into consideration and promoting for a better and safe way to keep everybody in their houses and not outside on kayaks in the middle of a hurricane?

DEBORAH ESCALERA: Okay. Go ahead. One last question.

UNIDENTIFIED MALE: I'd just like to make a comment according to what Savannah said, and a question for you because you know big data, you explore a lot of data from many parts and you process that, and the data itself contains sometimes bias and the outcome of this

bias in the data is being thrown at us into recommendation systems as Savannah mentioned earlier. So how do you see that in your research towards exploring trajectories or other types of data in your research?

JUAN A. FIGUEROA ROSADO: Yes. From the data we can actually extract from different communities, you would see, let's say, a region is very – let's just say this region loves going to the gym, and you're trying to extract meaningful information about medical issues in the region. So yes, the information could be heavily biased towards people going to the gym, and at the end, the program, could tell you, "No, they don't need a hospital nearby or a solution like that."

So in order to solve that, we would actually need to create an algorithm that removes – or as I mentioned, as the data gets passed to a neural network, let the neural network act with the sigmoid neurons that change the weight of different data that is being passed to the neurons as the data comes by. So you run the artificial data, and if you see that that data is being heavily biased, the network itself will modify so you can take into consideration that every aspect of the data that comes in is evenly represented in the results. That would be a good implementation of that.

Thank you for your question, that's very interesting.

DEBORAH ESCALERA: Okay. Thank you, Juan. Very interesting presentation. Well read. Okay, our next presenter is Allan Fret. Allan?

ALLAN FRET: Well, good afternoon. Like she said, my name is Allan Fret. I come from the University of Puerto Rico. I'm currently in my senior year of my bachelor degree. I was part of this research at Missouri University of Science and Technology. And the title of my presentation is A Secure Similar Document Comparison Protocol.

In ahead, I'm going to apologize because it's a little techie, the presentation. So hopefully, you are going to understand and I'll explain it as best as possible. This is the content of the presentation. We used some information retrieval techniques to compare the documents and their [inaudible] system to ensure the confidentiality of the information within the documents.

Secure document comparison has many applications in many fields. For example, in medical record comparison where if we want to compare – let's say that I'm a doctor and I have a patient who I might not know what disease the patient has and I want to compare the history of that patient to, let's say, Juan's

collection of patients. But revealing any information of the patient will break the law, and if he provides me any information of his patient, he will also be breaking the law.

So when we are doing comparison with documents, we need to ensure the confidentiality of the information, so that's where our secure document comparison protocol comes in. In this research ,what we did was we developed a client/server application where the client, let's say the doctor who wants to compare his patient to another doctor's collection, what the doctor does is, for example, he uploads the patient data of his patient and the protocol is going to encrypt, the application is going to encrypt all the information regarding his patient, and the document is going to be sent to the server side of the application where the application is going to do all the calculation between the two patients, and then at the end, the server side of the application is going to send all of the similarity scores.

So if there is a person, let's say, who is 99% similar to his patient, he can start a procedure to ask for the information of the other doctor without actually breaking the law or any privacy information regarding the other patient information.

So here, what we are doing is converting each and every document into a vector. The vector space model is an

information retrieval technique that a lot of people use. Each vector is going to be of M dimensions, where M is the size of all the documents of the server collection. So if the server has ten documents, each vector is going to be of M dimension.

And I said something bad. It's the size of unique words in the server collection. My bad. So if there are ten unique terms, then each vector is going to be of that dimension, and each vector element is a score for the corresponding term. We are assigning a [weight] to each term in the document.

So here is the TF-IDF that is the information retrieval technique. So what we are doing is we are taking the TF that basically does the term frequency. It's how many times does the term appear in that document. And the inverse document frequency, the IDF is 1+log(N/df.) DF means the document frequency. How many documents does that term appear in? That's the document frequency. And N is the size of the collection in the server side, is how many documents the server has, how many patients if we're talking about a doctor.

So what we want is the TF-IDF, is the multiplication of TF times IDF. And you may be asking yourself why we are using the TF-IDF instead of the term frequency. It's because if we are using the term frequency, we are not using the same weight for all the terms because all the terms have the same weight. For example,

if we are looking at documents of the automobile sector, we may have a word like auto, automobile that may appear in a lot of documents. So what the IDF does, if the term appears in a lot of documents, it gauges the term less significant because it appears more times.

And if we have a word like [inaudible] that may appear in only one document, what the IDF does is it assigns more weight to that term. So when we're multiplying the TF-IDF, we are taking that weight to that term, and we are taking in account the relative significance of words.

So here is where it becomes a little techie. We may have a dictionary of unique terms. Those terms are the ones that appear in at least one document in the server collection. So the server is going to create that dictionary of unique terms and is going to send it to the client where the client's going to create the document with the size of the dictionary. And what we want to do is to search for the TF-IDF of each term in the dictionary.

And you may be asking why we are using the terms in the dictionary. Because if you remember, the dot product, that's what we are going to use to calculate similarity within the vectors. It is similarity scores, the dot product, so we want to take into account only the words that appear in both documents. We don't want the words that only appear in one

document and in the other it doesn't. So that is why we are looking for the words in the dictionary in both documents to calculate the dot product.

So here is basically what the dot product is. And what we want to do, remember that we need to encrypt the information of the client. So let's say that vector one is the client document. So each cell in the client vector will be the terms. Each term in the client, in the vector one is going to be encrypted. So how do we actually do a comparison without knowing what the information is? Because each server is encrypted.

That is why we are using the pallier cryptosystem. I'm not going to get too deep in it, I'll just go on to explain the properties that the pallier cryptosystem has. It allows us to do mathematical calculations, and that is why we chose this pallier cryptosystem instead of RSA or other cryptosystems.

So we're going to use in this case the extended homomorphic properties to calculate the product of each cell. For example, what the extended homomorphic property says is that the encryption of a message raised up to the power of K [– for an unencrypted number K –] modn^2 is going to be equal to the encryption of both numbers multiplied together modn^2. So it will be the same as the encryption of the cell U_1 x V_1 and the product's going to be encrypted.

So we want to do that for each cell in both vectors. So what I'm trying to say is that the encryption of U_1 raised to the power of V_1 is going to be equal to the encryption of u_1 v_1. And if we take again the encryption of U_2 raised to the power of V_2 is going to be equal to the encryption of U_2 V_2.

But the result is going to be a vector with encrypted data in each cell, but we want the similarity score. We want a score like you're going to say, "Oh, okay." So we will have a score, and what we want to do after we multiply each encryption, we want to add the whole vector. We want to add each cell in the resolve vector so to be able to do addition of encrypted data, we are going to use the additive homomorphic property that says that the multiplication of two encrypted numbers is equal to the addition of the messages.

So we will have, for example, in the [result] vector the encryption of U_1 and V_1. In the second cell, we will have the encryption of U_2 V_2 and so on. So to be able to do the addition of the whole vector, we're going to multiply the encryption of U_1 V_1 times the encryption of U_2 V_2 times the encryption of U_3 V_3 and so on. And until you calculate the addition of [inaudible] that's going to be of how similar the two vectors are.

And I had a picture there of how the application looked like and the score of actual information of documents, and, well,

technical problems. If any of you want to see it, you can see it in my computer. And if you guys have any questions, hopefully I didn't… Okay.

DEBORAH ESCALERA: Thank you, Allan. Very good. Are there any questions for Allan? Audience first. No? Okay, let's start with the NextGen. We'll start from this side and then we'll go around the table. Go ahead.

JAMES WILSON: Hi. James Wilson, UCLA NextGen. I first wanted to know obviously your client applications. That seems like a really neat model. I really enjoyed your presentation, especially since from a stats background, seeing model building like that and encryption, I've never actually seen the mathematical background behind that before so it was really interesting. And I'd love to know your inspiration for using pallier and then how you think you can take this into the future with like document encryption and possible purposeful practices in our communities.

ALLAN FRET: So the first question was why we use pallier?

JAMES WILSON. Yes. Just like what was your inspiration.

ALLAN FRET: It was very good experience [inaudible] pallier cryptosystem because the properties allow us to do calculation with encrypted data. So that is why we didn't use for example RSA, because if you can look here, when you're multiplying encrypted data, it's basically the same as multiplying the data within the encryption. So if we have, let's say, message one is two and the encrypted message two is, let's say, two, when you multiply the two encryption, it's going to be the encryption of 4 modn^2. And the second question was –

JAMES WILSON: How you hope to use this in the future, either in your own community or just published practices.

ALLAN FRET: I was actually talking to one – I'm not sure how the policymaking in ICANN works right now because I'm trying to get in. so maybe in the future, if some individual is trying to make a policy, he actually could compare his policy, the policy that he's trying to make, to compare to a whole collection of policies made by ICANN, and he might be able to know if there is a policy that is more similar to his policy, and maybe in the future we can

improve the protocol by actually sending back the more similar document, but that's if he has the privilege to get to know the information. Because if there is a doctor and he is not allowed to see the information of the other person, then we are breaking the law.

DEBORAH ESCALERA: Okay. Next.

KAITLYN KARPENKO. Hi. Kaitlyn, NextGen. I found this really interesting. I do not have a very strong math background, so if my question was answered and I just didn't understand it, please feel free to tell me that. I have a two-part question. The first is, does this model account for contextual changes in meaning for words, or does it adjust for things like synonyms? Especially like in patient data, patients may describe their conditions differently so two identical conditions may be expressed very differently on paper.

And then my second question is regarding this comparison as a means of protecting the identity of the original sensitive documents and whether you've thought about the fact that you've actually provided a method for verification. So, for example, if you have a document and you want to know if that document is in a database, you can just run and see if you ever

get a 100% match which would verify that that document is in that database, which would be a major privacy concern. Like how do you address the privacy concerns with what seems like, to me, a verification model? If I don't understand it properly, then just let me know, but it seemed like a relatively easy way to either verify or verify that something isn't in the database that you're trying to find.

ALLAN FRET: Okay. The first question is basically we are just looking if both documents are similar. We are not taking into account what the person is meaning by that information. We're just checking if the words – like the terms in the document. We're not actually trying to figure out what it's trying to say, we're just comparing if the documents have the same types of words, basically. And the second question, can you say that again?

KAITLYN KARPENKO: Yes. So it seems like you've created a model where you can compare an encrypted document to a document you have without actually looking at the encrypted document. But it seems like you could theoretically compare a document you have against every encrypted document until you get a 100% match, thereby verifying that the document you have is in the database. For example, if you're trying to figure out if someone

has a specific condition, like if they're HIV positive, you know what an HIV positive medical record would look for for this person, so you go and collect the encrypted data for an HIV clinic and you just compare until you get a 100% match thereby verifying that this person is HIV positive.

ALLAN FRET: There is actually a research that my mentor did in that. I think the title of the research was A Secure [SKNN] Protocol that it calculates basically the – it converts the documents into vectors too but it calculates the Euclidean distance that it's [similarly close to]. But – I lost the question again. Okay.

KAITLYN KARPENKO: Sorry, can you repeat that?

ALLAN FRET: Like the question.

KAITLYN KARPENKO: Oh. So basically if I have a document and I'm looking for it in a database, can I just keep running this algorithm until I get a 100% match?

ALLAN FRET: Yes, we can. But if you have the access, you need to… For example, if I am the database, we need prior communication to connect the client side to the server side. So if I have the documents, with the application you can actually compare your patient in this case to the whole collection of documents that I have of the whole collection of patients that I have.

KAITLYN KARPENKO: Right, so my question is basically, couldn't this be used as a privacy violating tool? Because if you have a document and you're trying to figure out if it's contained within a dataset that's otherwise encrypted, you can now verify whether this document is contained within this dataset, which would thereby be an identifying way [inaudible].

ALLAN FRET: Yes, but we're not actually revealing any information of the server side.

KAITLYN KARPENKO: But you would be, because if you return a 100% match, it reveals something about the document you have.

ALLAN FRET: Yes, but you don't actually know the information of the document. You submit your document, it encrypts all the unique terms, but in any case, the server side is actually revealing how many documents does the server has or the information regarding the documents. You only know that he has a document that is 100% or 60% similar to yours. So if you actually want to see the documents, you need to talk to the person and start the process, basically.

KAITLYN KARPENKO: Right. I think you're missing – sorry, the point of the question is you have a document, and you want to know if the dataset you're working with which is encrypted and highly sensitive contains the document you have, because it would verify information or identity or something for you. Like let's say you want to know where Jane Smith lives, and you have a piece of document.

You know Jane Smith is in this dataset, you know certain things about her, and you know this document is associated with her. But if she isn't in this dataset, then it's not associated with her. So you can thereby run your model, get a 100% match and thereby verify that the information you have pertains to Jane Smith. Does that make sense? We can talk offline later.

ALLAN FRET: I can [inaudible]. Yes, okay. I want to say something I guess.

DEBORAH ESCALERA: [inaudible] Because now we're out of time and we need to move on. Sorry. Our next presenter – it's Sarah Ingle. Sorry. I apologize, NextGen. If you want to ask Allan further questions on his presentation, please do afterwards. Thank you, Allan. [Very well]. Okay.

Our next presenter, our final presenter is Sarah Ingle, and I want to make sure that she has some time for questions, so let's move on. Sarah?

SARAH INGLE: Thank you very much, everyone, for prefacing with such fantastic presentations. It's really been a privilege to hear from all of you today, so I'm glad to be able to end the session as well. So the topic of my presentation is working towards an Internet of representation and thinking about incorporating diversity and inclusion into both the processes of tech and governance development.

To provide a little bit of a background about me – if it stops twitching – I'm a student in international relations at Trinity College in the University of Toronto. I'm Canadian and British. I grew up in Waterloo, Ontario, which is very much one of the tech

hubs of Canada. We're home to companies like Blackberry as well as the Canadian Google headquarters. And so discussions about technology and the way that it intersects with our daily lives has been a part of my life from a very young age.

So then going into my studies at the University of Toronto, I very much had an interest in the intersections of digital innovation, cybersecurity, human security and international law. Something that I think about a lot particularly is how the terms of cybersecurity and human security can perhaps come closer together in the future and one can help us understand the other.

I'm here mainly however in my capacity as the ambassador for the youth IGF in Canada. We're essentially an initiative that has started in the past year and is a part of the broader youth IGF movement, a sponsored initiative of the United Nations IGF and we're housed under kind of a broader organizations called Together Against Cybercrime International which is an NGO based in France. So we work in partnership actually with ICANN and others to focus on educating youth on Internet governance and technological policy issues, as well as giving them opportunities to actually participate in these discussions. So I commend ICANN particularly for having us all here and for hosting such fantastic programs like NextGen and the Fellowship.

Recently, my work has involved posting a community forum. When I found out that I would be participating in this program, I wanted to give students in Canada the opportunity to actually kind of essentially script me and say, "Here's what I want to have you share at ICANN." And so we hosted this forum very recently on March 1st. This was actually in collaboration as well with The Citizen Lab at U of T which is a very prominent research organization focused on digital security issues and human rights.

So our session began actually with a presentation of their new personal security program which is called Security Planner, and I encourage all of you to test out this tool and to actually get in touch with The Citizen Lab and give them any recommendations you may have. It's a tool that's both for high-risk and low-risk individuals, and it's for developing kind of better security practices for everyone in the hope of, as I said, creating better digital security as a network process. So the fact that if we each change our habits, we will also by extension improve the security of all those we are connected to.

So following from that, we hosted a discussion and a consultation period, and this involved students, mainly in their undergraduate degree at U of T from students in international relations as well as computer science, economics and a variety of other disciplines, and across several years of study.

So there were several key outcomes of this discussion, and I can kind of group them broadly into five themes and two questions. All of this has actually been put into a summary document that provides a lot more detail on kind of commentary and overview of the session as well, and you can find that on our Facebook page.

But generally, in discussing themes like privacy, culture, security, accessibility and intervention, we arrived at two questions broadly, and that was, "Is the Internet uniting or dividing us, and how do we govern the Internet?" The uniting or dividing us question came up at the very beginning because we've all been very avidly following changes pertaining to net neutrality. And something that many students expressed is concern over the way that this sort of stratifies access to information within societies, and also situating that within the context of all of our usage of social media as well.

And so a principal concern that was brought up too is the design of social media and its algorithms in the way that the information you experience is very much based on your circles of association and in that way can kind of create just a personal echo chamber. So we were thinking about the ways that social media and things like net neutrality affect diversity of thought and in turn how this may affect our political systems going forward.

So bridging from that and kind of venturing through some of those topics in-between, we then at the end just posed the simple but not so simple question of, "How do we govern the Internet?" And our group came up with three levels of analysis, broadly.

Firstly, obviously things to do with data and information security are going to affect national policies, and so it's important that capacity be developed in terms of domestic regulations, and a lot of countries are really moving forward with doing this recently. Canada actually just committed in the new budget I think it was $50 billion or $500 billion potentially – it was a substantial figure anyhow – towards building our cybersecurity capacity.

So that's one tier. But as well, it's exceptionally important to have things like ICANN and the IGF and to be having conversations at a global level where we kind of put these policies in contrast with one another and also think about how we can develop global standards. But another thing which came up was – and obviously, ICANN is a huge advocate of this, but – thinking about the Internet users themselves.

One of the students participating is actually from a country with quite restrictive Internet policies, so they were kind of giving a testimony of their experiences with free speech online. And

something that they and others pointed out was thinking about individual empowerment as a means of shifting policies. And thinking about tools such as free VPNs or other encryption tactics which would enable people to freely express themselves and sort of start policy change in the country from the bottom up by, again, putting kind of that tool in the pockets or on the laptops of people.

So bridging from this, the topic – as we were considering each of these levels of analysis, we started thinking as well about the major pitfalls of each. And representation, especially with our discussions on culture, was one of the issues which came up most prominently. So I would like to sort of focus on the IGF a little bit in this next segment but highlight two areas in which I think diversity and inclusion could be substantially improved.

So firstly, and speaking as a woman as well, the problem of gender in Internet governance is very substantial. These figures here are from – one is from the Internet Governance Forum on their most recent attendance program statistics, but the other one is some work that the Diplomacy Foundation did on gender participation in Internet governance.

And so the first shows gradually an improvement in conversions of gender participation in Internet governance at the IGF, and the second kind of breaks those down as well, but there hasn't

been very much substantial change, and one of the most interesting statistics as well which comes from the Diplomacy foundation's work was on not just presence but participation, and so it was breaking down female participation in terms of the words spoken and actually participation in discussion, and these figures were often substantially worse than just the presence.

Secondly, I find it's very interesting to look at the evolution of stakeholder groups within the IGF. I'm just going to highlight two elements here which I think are important, but since its inception, the presence of media at the IGF has become substantially reduced. I find that very problematic because if we don't have sort of press presence at these events and an engagement with global narratives, it becomes, again, a potential echo chamber for similar thought. And secondly, there's been a massive expansion of civil society, but private sector participation has diminished as well. And that is partially because I think there's a frustration in tech companies with sort of gradualist diplomatic processes.

And I was just speaking with a connection of mine at Microsoft who confirmed all of this because Microsoft is definitely a company which is focusing increasingly on developing internal capacities for policy creation as well. So that's something that I think in the years going forward it is absolutely crucial that we pay attention to and we focus on new ways to continue

improving private sector participation, and making those pie graphs a little bit more distributed.

So this brings me to kind of my closing points, but when we think about diversity and inclusion in Internet governance, I think we need to shift from not just talking about involvement but speaking about representation. And as a representative earlier from the ICANN org said, I think we're very privileged to be in a place here where we can participate more actively, but this is definitely not the case across the board. And so where we don't have equal representation in Internet governance, we fall prey to a lot of the biases which have come up in a lot of other presentations today, and so that's happening in terms of not only governance and the issues that are brought to the table in the first place but in technology, kind of inherent bias that's programmed in. And we've all read articles as well on kind of problems with that for facial recognition amongst other technologies. But lastly, we definitely need to work on making education more equally available and focusing particularly with attention to the gender dimension on promoting not only more female involvement but also encouraging speaking between disciplines. The technical political divide, as we all know, is very real, and I think when we are hoping to deal with some of the issues which arose with big data for one, we need to improve the

capacity for people to speak with one another. And so that's a piece about collaborative integration as well.

And so representation is important to the initial question of how do we govern the Internet, because it's also about ending the echo chamber and bringing in a variety of perspectives which will change the very nature of the conversations we have. So looking forward with what this means for my work in a practical sense, in fall of 2018, we will be organizing the first Canadian Internet Governance and Digital Policy Forum, and this is intended to – it will be with the IGF but also in partnership with a variety of Canadian ICT companies as well as civil society and Citizen Lab likely, but this will be an opportunity for youth to not only just be kind of a token presence as sometimes occurs but to actually participate and be in discussion with the members of various Internet governance organizations and with the technical policy advisors within companies themselves.

And so the aspiration for this event will be to actually develop an outcome document which states Canadian youth and interest holders' kind of perspective on Internet governance and encapsulate this and use this as a policy tool for advocacy at a government level. Further to this, we will be focusing also very heavily on educational initiatives and on bridging the technical political gap within the University of Toronto and across educational communities in Canada as well.

I'd be more than happy to talk about this in further depth. I'm also happy to speak to you about how you can start these initiatives in your own countries. We are looking to expand and we currently have a very strong network across Africa, the Middle East and Europe, but North America is, sure, there's room for improvement. So thank you very much.

DEBORAH ESCALERA: Thank you. We have exactly two minutes because there's another group scheduled to be in this room, so Ishan, we're going to take just two questions. So Ishan at the end.

ISHAN MEHTA: Hello. Yes. This is Ishan from NextGen. Very quickly, two points: the Humane Society in San Francisco is like a bunch of former Silicon Valley developers who are now sort of railing against the machine, and they did a cool gender disparity study on – it's not just participation but it's also leadership [inaudible] roles, and I think today's morning opening ceremony was a sort of testament to that, that even if you have women turn up, how many of them are actually in panels, how many of them are actually speaking, how many of them are actually chairing committees makes a bigger difference. So I think I just mansplained gender diversity there.

And the second point I was going to make is that I also lead a digital rights group in Atlanta, and I don't know if this is your experience, but have you seen this big difference between the undergrads who grew up with the Internet and people like me in grad school who still remember dialup? The things we care about, I don't know if that's – I don't want to say generational because it's like five years, but a timeline difference, or is it more of me being so entrenched in this world versus them just viewing the Internet as a tool or an accessory?

SARAH INGLE: Thank you very much for your questions and for those connections to different organizations. I think you're absolutely right, actually, and it is sort of weirdly a generational divide that I think happens a lot quicker now than it used to. Just with the speed and the rapidity of technological innovation, I think it's very possible for people just a few years apart to have very different perspectives on technology.

And one of – I think – the problems that I have faced in getting people involved in this initiative is very much that my peers are completely used to having the Internet just be a part of every single moment of their daily lives and being completely kind of open and willing to have their data disclosed and collected by various organizations. So kind of creating a little bit of

discomfort is something that I'm striving towards, I guess, but I think you're absolutely right. And it would be fantastic to kind of try and think about how we can maybe have that slightly older generation help bring that conversation to people a few years younger.

DEBORAH ESCALERA: Okay. One last brief question. Savannah?

SAVANNAH BADALICH: I guess it'll just be a comment, and then depending on how much time, we can just talk offline. But totally agree about the parity conversation, the representation. I also worry about when we talk about representation we're just talking about checking boxes, so even gender parity in a space like this, having conversation around norms and stereotypes that go with it, because we can have equal numbers of people at the table, but if we still have preconceived notions of each other, it makes it very hard for someone to feel comfortable to talk.

But just a question around trust. How are these young people – what is their sense of trust with technology right now, considering everything that's going on? Did you glean anything about that from your community forum?

SARAH INGLE: I think it's changing a bit more recently as these topics come into the public domain a bit more. I'm always shocked by the fact that Bitcoin was a part of a very select group of people's vocabulary just over a year ago and it's now sort of in the headlines 24/7, I think that's a testament to the fact that those perspectives can change and are potentially underway and they're changing. But I think we are far more trusting than we should be, and there is sort of a tradeoff that people are very comfortable with currently of, "I realized that I can't live without my laptop, my phone, my this, my that and so I recognize these things are bad, but is it really hurting me on a daily basis."

People talk a lot in sort of environmental concerns as well about like distanciation from a problem, and I think technology in the fact that it's not so tangible sometimes can make people a lot more disconnected, and particularly people who are used to having the Internet pervade their lives, it just creates a level of unconscious comfort, I would say, an implicit trust.

DEBORAH ESCALERA: Okay. Thank you, Sarah. Wonderful presentation. Okay, so I want to thank all the NextGen who presented today and remind audience members and the remote participants that we do have another session tomorrow, more presentations tomorrow. And thanks to everybody.

[END OF TRANSCRIPTION]